UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/792,325	03/02/2004	Mauricio Sanchez	200316381-1	4396

22879 7590 10/16/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
JEAN GILLES, JUDE	
ART UNIT	**PAPER NUMBER**
2443	

NOTIFICATION DATE	DELIVERY MODE
10/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/792,325	SANCHEZ, MAURICIO	
	Examiner	Art Unit	
	JUDE J. JEAN GILLES	2143	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-49* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-49* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is responsive to communication filed on 03/02/2004.

Response to Amendment/arguments

1. Claims 1, 12, 23, 34, 39, and 44 have been amended. Applicant's arguments, filed 07/07/2008, with respect to the rejection(s) of claim(s) 1-49 under Dent and Tzamaloukas have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Smith and Narsinh.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. **Claims 1-5, 12, 20-22, and 34** are rejected under 35 U.S.C. 102(e) as being anticipated by Smith et al (hereinafter Smith) U.S. App. No. 2008/0055158 A1.

Smith teaches:

1. A computing device, comprising:

a processor (fig. 6 item 660);

a memory coupled to the processor (fig. 6, items 660 and 670); and

program instructions provided to the memory and executable by the processor (par. 0102) to:

transmit a network management message, using one of simple network management protocol (SNMP) or internet control message protocol (ICMP), over a network to a network device (par. 0116; note the system sending and alert or alarm messages using the SNPM protocol);

collect response information from the network device based on the network management message (*par. 0118; see the role of the transceiver that when deployed report measurement results to position engine 110 for instance, in response to alerts and/or alarms*); and

analyze the response information including applying a Kalman filter to the collected response information (par. 0167, 0169, and 0171).

2. The device of claim 1, wherein the computing device is a network event regulator device (par. 0063, 0085, and 0095).

3. The device of claim 2, wherein the computing device is selected from the group of a wireless access point, a switch, a hub, and a router (see access points 180A-B; par. 0049).

4. The device of claim 1, further including program instructions which execute to regulate external network stimuli based on applying the Kalman filter to reduce

degraded performance to the network (par. 0167, 0169, and 0171; note the use of the retrain model in par. 0169).

5. The device of claim 1, further including program instructions which execute to signal when abnormal levels of activity are detected based on applying the Kalman filter (par. 0167, 0169, and 0171; note that Kalman filtering performs a weighted average of the measurements, controlling and detecting abnormal levels of activity).

12. A computing device, comprising:

a processor (item 660);

a memory coupled to the processor (items 670 coupled to item 660); and

program instructions provided to the memory and executable by the processor (par. 0102) to:

collect traffic flow amount information from a network device connected to the computing device over a network (par. 0102; see also par. 0100, and 0101 in which is disclosed that "*Bridge 640 may be used to transfer traffic from mobile devices through WLAN 620 to any network connected to network interface 650, which may use an alternate network such as a wired network or an alternate wireless network*." As the bridge 640 monitors traffic it also inherently controls traffic flow from the from WLAN 620 to network interface 650);

analyze collected information including applying a Kalman filter to the collected response information (par. 0167, 0169, and 0171); and

limit amount of traffic flow through the network device based on applying the Kalman filter to reduce degraded performance on the network (par. 100-102, and par. 0167, 0169, and 0171; As the bridge 640 monitors traffic it also inherently controls and limits traffic flow from the from WLAN 620 to network interface 650).

20. The computing device of claim 12, wherein the network device includes a network device selected from the group of: a switch; a hub; a database; a security appliance; a wireless access point device; a network intrusion device; and a router(see access points 180A-B; par. 0049).

21. The computing device of claim 12, wherein the network device and the computing device are connected over a local area network (LAN) (par. 0049, 0056, and 0066).

22. The computing device of claim 12, wherein the network device and the computing device are connected over a wireless wide area network (WAN) (par. 0049, 0056, and 0066).

34. A method for network and network device management, comprising:

collecting information associated with a network device (Smith; *par. 0118; see the role of the transceiver that when deployed report measurement results to position engine 110 for instance, in response to alerts and/or alarms*);

analyzing the collected information including applying a Kalman filter to the collected information (Smith; *par. 0118; see the role of the transceiver that when deployed report measurement results to position engine 110 for instance, in response to alerts and/or alarms*); and

regulating external network stimuli based on applying the Kalman filter in order to reduce network performance degradation (par. 100-102, and par. 0167, 0169, and 0171; As the bridge 640 monitors traffic it also inherently controls and limits traffic flow from the from WLAN 620 to network interface 650).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 6-8-11, 13-19, 23-33, 35-38, and 35-49** are rejected under 35 U.S.C. 103(a) as being unpatentable over Smith in view of Narsinh et al (hereinafter Narsinh) U.S. App. No. 2005/0201415 A1.

Regarding claim 6, Smith teaches a Kalman filter with instructions capable of collecting and analyzing network management information, but fails to specify that the collect of network information includes the step of tracking media access control (MAC) layer addressing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network. Nevertheless, this feature is well known in the art as evidenced by Narsinh.

In the same field of endeavor, Narsinh teaches that MAC addresses are matched in the MAC address tables in an egress and ingress switching device, matching the MAC addresses using the layer 2, a well known process in the art (see Narsinh, par, 0016). Using this technique will facilitate the system in the process of collecting, comparing and analyzing network management information,

Accordingly, an average skill in the art, would be motivated in incorporate the system of Smith, means of maintaining the advantages reducing the computational demands on the network processor, allowing for improved throughput in switching devices in which the network processor bandwidth is oversubscribed as stated by Narsinh, par. 0003-0004. By this rationale, claim 6 is rejected.

Regarding claims 7-8-11, 13-19, 23-33, 35-38, and 35-49, the combination Smith-Narsinh teaches:

7. The device of claim 1, further including program instructions which execute to track internet protocol (IP) flow and routing and which execute to learn network events based on applying the Kalman filter as other devices connect to the network (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0016, and 0022).

8. The device of claim 7, further including program instructions which execute to track IP flow and routing at a network device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router (Smith; see access points 180A-B; par. 0049).

9. The device of claim 1, further including program instruction which execute to track information between various network layers in a given protocol stack model and which execute to learn network events based on applying the Kalman filter to the tracked information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

10. The device of claim 9, wherein the various network layers include network layers in a protocol stack model selected from the group of: an OSI protocol stack model; an SS7 protocol stack model; and a TCP/IP protocol stack model (Narsinh, par. 0013, and 0016).

11. The device of claim 9, wherein the various network layers include network layers selected from the group of: a TCP port-level connection; a session level connection; a

presentation level connection; an application level connection; a transaction capabilities application part level (TCAP) level connection; an integrated services digital network user part (ISUP) level connection; a mobile application part (MAP) level connection; and a signaling connection control point (SCCP) level connection (Narsinh; par. 0056).

13. The computing device of claim 12, further including collecting information from the network device selected from the group of: processor utilization; memory utilization; link up/down status; traps; buffer utilization; local area network (LAN) utilization; and statistics including discards, cyclical redundancy checking (CRC) and frame check sequence (FCS) errors and number of broadcasts (Narsinh, par. 0020).

14. The computing device of claim 12, further including program instructions which execute to automatically calibrate a threshold in the network device used to control a connection rate to the network device (Narsinh, par. 0050-0052).

15. The computing device of claim 14, further including program instructions which execute to convert the network device to perform a different role (Narsinh, par. 0050-0052).

16. The computing device of claim 15, further including program instructions

which execute to convert a network database to serve as a network hub (Narsinh, par. 0050-0052).

17. The computing device of claim 15, further including program instructions which execute to convert a network switch to a network hub (Narsinh, par. 0050-0052).

18. The computing device of claim 12, further including program instructions which execute to track media access control (MAC) layer addressing and, based on applying the Kalman filter, execute to reduce false positives and false negatives (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0016, and 0022).

19. The computing device of claim 12, further including program instructions which execute to track internet protocol (IP) flow and routing and, based on applying the Kalman filter, execute to reduce false positives and false negatives (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0016, and 0022).

23. A method for network and network device management, comprising:

receiving network information associated with a network device (Smith; *par. 0118; see the role of the transceiver that when deployed report*

measurement results to position engine 110 for instance, in response to alerts and/or alarms); and

analyzing the network information using a Kalman filter (see Smith; par. 0167, 0169, and 0171); and

wherein the network information includes media control (MAC) layer addressing and internet protocol flow and routing information (Narsinh, par, 0016). The same reason to combine and motivation used for the rejection of claim 6 is also valid for this claim. By this rationale, claim 23 is rejected.

24. The method of claim 23, wherein the method includes receiving response information to an SNMP message sent to the network device (par. 0116; note the system sending and alert or alarm messages using the SNPM protocol).

25. The method of claim 23, wherein the method includes receiving information contained in a management information base (MIB) of the network device (see Smith, item 1910).

26. The method of claim 23, wherein the method includes using a software agent embedded in the network device to receive and analyze the network information (Narsinh; par. 022, 0025, and 0054).

27. The method of claim 23, wherein the method includes receiving network

information associated with a device selected from the group of a switch, a hub, a database, a security appliance, a wireless access point device, a network intrusion device, and a router(Smith; access points 180A-B; par. 0049).

28. The method of claim 23, wherein the method includes receiving media access control (MAC) layer addressing information (Narsinh, par, 0016).

29. The method of claim 23, wherein the method includes receiving internet protocol (IP) flow and routing information (Narsinh, par, 0016).

30. The method of claim 23, wherein the method includes: receiving information communicated between various network layers in a given protocol stack model; and learning network events based on applying the Kalman filter to the received information (Narsinh, par. 0013, and 0016).

31. The method of claim 23, wherein the method includes reducing false positives and false negatives based on applying the Kalman filter to received network information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

32. The method of claim 23, wherein the method includes regulating external network stimuli based on applying the Kalman filter to received network

information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

33. The method of claim 23, wherein the method includes producing an alert signal when abnormal levels of activity are detected based on analyzing the network information using the Kalman filter (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

35. The method of claim 34, wherein the method includes receiving media access control (MAC) layer addressing information and learning network events based on applying the Kalman filter to the MAC layer addressing information Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

36. The method of claim 34, wherein the method includes receiving internet protocol (IP) flow and route information and learning network events based on applying the Kalman filter to the IP flow and route information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

37. The method of claim 34, wherein the method includes converting the network device from a first role to a second role based on applying the Kalman filter to the collected information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par.

0013, and 0016).

38. The method of claim 34, wherein the method includes automatically calibrating a threshold in the network device used to control a connection rate to the network device based on applying the Kalman filter to the collected information while the network device is in network use (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

39. A computer readable medium having instructions for causing a device to perform a method, comprising:

receiving network information associated with a network device (par. 0116-0118); and

analyzing the network information using a Kalman filter (par. 0167, 0169, and 0171); and

wherein the network information includes media control (MAC) layer addressing and internet protocol flow and routing information (Narsinh, par. 0013, and 0016). The same motivation and reason to combine used for the rejection of claim 6 is also valid for this claim.

40. The medium of claim 39, wherein the method further includes automatically calibrating a threshold in the network device used to control a connection rate to the network device based on applying the Kalman filter to the network

information while the network device is in network use device (Narsinh, par. 0050-0052).

41. The medium of claim 39, wherein the method further includes learning media access control (MAC) layer addressing events based on applying the Kalman filter to MAC layer addressing information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

42. The medium of claim 39, wherein the method further includes learning internet protocol (IP) flow and routing events based on applying the Kalman filter to IP flow and route information(Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

43. The medium of claim 39, wherein the method further includes converting the network device from a first role to a second role based on applying the Kalman filter to received network information (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

44. A network device, comprising:

a processor (Smith; fig. 6 item 660);

a memory coupled to the processor (Smith; fig. 6, items 660 and 670);

means for limiting amount of traffic flow through the network device based on applying a Kalman filter to information associated with the network device (par. 100-102, and par. 0167, 0169, and 0171; As the bridge 640 monitors traffic it also inherently controls and limits traffic flow from the from WLAN 620 to network interface 650).

45. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on the network device (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

46. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes executing a set of program instructions on another network device connected to the network device over a local area network (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

47. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to convert the network device to a different role (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

48. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to

reduce network performance degradation on the network device (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

49. The device of claim 44, wherein the means for regulating external network stimuli based on applying the Kalman filter includes program instructions which execute to reduce network performance degradation on a different network device (Smith, par. 0116, 0167, 0169, and 0171; Narsinh, par. 0013, and 0016).

Conclusion

6. ***This action is made Non-Final***. Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger, can be reached on (571) 272-4. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-3301.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-0800.

/Jude J Jean-Gilles/

Primary Examiner, Art Unit 2143

October 08. 2008